UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,841	06/13/2000	James L. Jason, Jr.	219.38418X00	5195

7590 02/24/2004

Blakely, Sokoloff, Taylor & Zafman LLP
c/o Grace Abercrombie
1279 Oakmead Parkway
Sunnyvale, CA 94086

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 02/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/592,841	JASON, JR., JAMES L.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 10 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 10, it recites the limitation "the application" in lines 4-5 of the claim. There is insufficient antecedent basis for this limitation in the claim.

b. Regarding claim 12, it recites the limitation “a network unit” in the first line of the claim. It is not quite clear as to what the limitation refers to.

Claim Rejections - 35 USC § 103

4. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Attwood et al. (6,347,376) in view of Nikander et al. (6,253,321).

a. Regarding claims 1, 20 and 28-29, Attwood disclose a method comprising:

monitoring application socket requests (col. 3, lines 34-40; col. 8, lines 57-59);

requesting a TCP connection by an application (col. 3, lines 34-40; col. 8, lines 57-59);

determining if there is security rule information binding, which meets the limitation of an active security association, that exists to protect network flow associated with the connection request (step 1102, fig. 11 and col. 3, lines 34-38);

preventing the connection request from proceeding if no active security association exists to protect the network flow (steps 1108, 1112; fig. 11);

determining if a security policy exists for the network flow if no active security association exists to protect the network flow (steps 1108, 1112; fig. 11);

allowing the connection request to proceed if one of the active security association exists (step 1110, fig. 11).

The Attwood reference does not disclose whether the security association for each security policy is manually configured or dynamically negotiated, and therefore, does not disclose the step of alerting a security association negotiation component to initiate negotiation for a security association based on the security policy if the security policy exists for the network flow, and using the security association established from the negotiation in the step of allowing the connection request to proceed. Nikander discloses a key manager using the ISAKMP/Oakley protocol, which meets the limitation of the security association negotiation component; and the step of a policy manager alerting the key manager to negotiate a security association for a connection based on the security policy when the first packet is examined (col. 4, lines 38-40; col. 5, lines 33-40; col. 6, lines 33-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Attwood to use a security association negotiation component, a policy manager, and to include the step of alerting

a security association negotiation component to initiate negotiation for a security association based on the security policy, as suggested by Nikandar, so that a security association can be negotiated as needed for IPsec processing.

b. Regarding claims 2 and 21, the security association negotiation components in those claims use the ISAKMP/Oakley protocol, which meets the limitation of the IKE component.

c. Regarding claim 3, Attwood further discloses that the active security association and the security association are based on at least one of a source IP address, a destination IP address, a protocol, a source port, and a destination port (col. 6, lines 13-18).

d. Regarding claim 4, Attwood further discloses that the protocol comprises one of TCP, UDP, ICMP, and IGMP (col. 6, lines 22-23).

e. Regarding claim 5, it is interpreted as "determining if the network flow can be allowed if the packet matches a filter in which the corresponding action states to allow the traffic to flow in the clear" (see fig. 3, step S19; and page 11, lines 2-5). Attwood further discloses that a packet is allowed if IPSEC is not required (fig. 8, step 812).

f. Regarding claim 6, Attwood further discloses retrieving the security association from a database (col. 6, lines 40-42).

g. Regarding claim 7, Attwood further discloses that the database contains mapping between network flow information and security associations (fig. 5).

h. Regarding claim 8, Attwood further discloses that the network flow information comprises at least one of a source IP address, a destination IP address, a protocol, a source port, and a destination port (col. 6, lines 13-18).

i. Regarding claim 9, Attwood further discloses retrieving the security policy from a database (fig. 5).

j. Regarding claims 10-12 and 24-26, Attwood disclose a method comprising:

monitoring application socket requests (col. 12, lines 7-12);

requesting transmission of UDP data on a socket by an application (col. 12, lines 7-12);

determining if the socket has been associated with a security rule information binding, which meets the limitation of an active security association (col. 4, lines 4-17 and step 1302, fig. 13);

determining if there is a defined security association that may be used to protect the network flow if the socket has not been associated with any active security association (step 1312, fig. 13);

allowing the UDP data to be sent if a defined security association is determined (step 1310, fig. 13).

Attwood does not disclose the steps of: determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow; alerting a security association negotiation component to initiate negotiation for a security association using security parameters specified by the security policy if the security

policy exists for the network flow; and establishing the security association. Nikander discloses a policy manager, the policy manager determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow (col. 4, lines 60-64; col. 6, lines 26-32); a key manager using the ISAKMP/Oakley protocol, which meets the limitation of the security association negotiation component; and the step of a policy manager alerting the key manager to negotiate a security association using security parameters specified by the security policy and establishing the security association (col. 4, lines 38-40; col. 5, lines 33-40; col. 6, lines 60-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Attwood to use a policy manager and a key manager, and to include the steps of determining what security policy should be used when negotiating a security association for the network flow if there is no defined security association that may be used to protect the network flow; alerting a security association negotiation component to initiate negotiation for a security association using security parameters specified by the security policy if the security policy exists for the network flow; and establishing the security association, as suggested by Nikandar. The motivation for doing so would have been to negotiate and establish a security association as needed for IPsec processing.

j. Regarding claim 13, Attwood further discloses that the second determining comprises comparing filters with at least one of a source IP address, a destination IP

address, a source port, and a destination port related to the network flow (col. 6, lines 13-18).

k. Regarding claim 14, Attwood further discloses that each filter comprises at least one of a source IP address, a destination IP address, a protocol, a source port, and a destination port (col. 6, lines 13-18).

l. Regarding claim 15, Attwood further discloses that the security policy comprises one filter (fig. 5).

m. Regarding claim 16, it is interpreted as "determining if the packet can be allowed to be transferred in the clear without a security association" (see fig. 5, step S34; and page 12, lines 3-5). Attwood further discloses that a packet is allowed if IPSEC is not required (fig. 8, step 812).

n. Regarding claim 17 the limitation "a network unit" in the second line of the claim is interpreted as "a communicating peer" (see page 2, lines 17-18). Attwood discloses a computing device comprising:

a network interceptor, the network interceptor monitoring an application's socket request (col. 3, lines 34-40; col. 8, lines 57-59; col. 12, lines 7-12);

a security association database operably connected to the network interceptor, the security association database containing a mapping of network flow information to security association information (col. 6, lines 40-42);

a security policy database operably connected to the network interceptor, the security policy database containing policies that describe parameters that are to be used in a negotiation of a security association (fig. 5);

an Internet Protocol security packet classifier, the IPsec packet classifier responsible for performing IPsec processing on incoming and outgoing packets (fig. 8),

Wherein the network interceptor insures that a security association is in place before allowing network traffic to flow between the application and the network unit (fig. 11).

Attwood does not disclose a security association negotiation component operably connected to the network interceptor, the security association negotiation component capable of negotiating a security association with a network unit. Nikander discloses a key manager component using the ISAKMP/Oakley protocol, which meets the limitation of the security association negotiation component; the key manager component capable of negotiating a security association with a network unit (col. 4, lines 38-40; col. 5, lines 33-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the device of Attwood to include a security association negotiation component capable of negotiating a security association with a network unit, as suggested by Nikandar, so that a security association can be negotiated as needed for IPsec processing.

o. Regarding claim 18, Attwood further discloses that the network flow information comprises at least one of an IP addresses, protocol, ports (col. 6, lines 13-18).

p. Regarding claim 19, the security association negotiation component in claim 17 uses the ISAKMP/Oakley protocol, which meets the limitation of the IKE component.

q. Regarding claim 22, Attwood does not disclose negotiating for a security association using security parameters specified by a policy. Nikandar discloses that the

key manager component negotiates for a security association using security parameters specified by a policy (col. 5, lines 33-37; col. 6, lines 60-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Attwood to include negotiating for a security association using security parameters specified by a policy, as suggested by Nikandar, so that security associations can be correctly negotiated as required by security policies.

r. Regarding claim 27, Attwood does not discloses that the active security association comprises a security parameter index (col. 6, lines 40-42), which comprises at least one of a source IP address, a destination IP address, a protocol, a source port, and a destination port.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ylonen et al. (6,438,612) disclose a method and arrangement for secure tunneling of data between virtual routers.

Engel et al. (6,519,636) disclose a method for controlling and manipulating network transmission by associating network flows with rule-based functions.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Minh Dinh
Examiner
Art Unit 2132

MD
02/19/2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100